Seguridad en el comercio electrónico

José Antonio Labodía Bonastre
Director de Seguridad.
joseantonio.labodia@securitas.es

Este artículo es un resumen de la ponencia del mismo título presentada en el I Congreso de ACTA, que se celebró en el marco incomparable de la ciudad de Sevilla los días 29, 30 y 31 de octubre. A lo largo de él vamos a intentar responder a estas cinco preguntas.

1. ¿Qué es el comercio electrónico?
2. ¿Qué problemas de seguridad presenta en la actualidad?
3. ¿Qué soluciones existen?
4. ¿Cuál es la solución idónea? ¿Las técnicas de cifrado?
5. ¿Cuáles son los estándares de seguridad en el comercio electrónico?

Seguidamente vamos a desarrollar todas y cada una de estas cuestiones planteadas más arriba y responder a algo más cotidiano: ¿Es seguro enviar nuestro número de tarjeta de crédito por la Red?

1. ¿QUÉ ES EL COMERCIO ELECTRÓNICO?

El comercio, la actividad comercial, es algo consubstancial al ser humano. ¿Cuándo nació? No se sabe a ciencia cierta. Su nacimiento está perdido en la noche de los tiempos, como tantas otras actividades humanas. En algún momento del periodo neolítico alguien pensó que no era una idea descabellada cambiar algo, que interesaba a otra persona, por algo que esta persona tenía y que le interesaba a él. Estos dos individuos habían sentado los cimientos del comercio, iniciándose con el trueque de productos - fundamentalmente agrícolas -. Como toda actividad humana, fue evolucionando y basándose, a través de los siglos, en diversos sistemas de intercambio, hasta llegar al invento del dinero como medio de pago. Lógicamente, esta evolución natural ha llegado hasta nuestros días, desarrollándose junto con los nuevos medios que ofrecen las redes de comunicaciones y las tecnologías de la información.

Pero, ¿Qué se puede considerar en la actualidad como comercio electrónico? Una definición podría ser perfectamente la siguiente: "*Comercio electrónico es toda aquella actividad comercial en la que las operaciones de compra/venta y/o el pago de los bienes o servicios adquiridos se realizan a través de medios electrónicos*".

Indudablemente el comercio electrónico tiene un gran potencial de desarrollo y el cauce idóneo para su definitiva materialización es, sin ninguna duda, Internet. El comercio electrónico representa las siguientes facilidades para las dos partes que intervienen en el mismo:

PARA EL VENDEDOR	PARA EL COMPRADOR
Mayor número de potenciales clientes. (*Todos los internautas del mundo*)	**Comodidad.** (*La transacción se realiza desde el propio domicilio*)
Más disponibilidad, menor coste. (*Sin stocks, ni almacenes*)	**Facilidad de compra y selección de productos.** (*Utilizando el ratón, se pueden ver todos los productos expuestos en la página*)
Sin costes físicos. (*El producto se pide al proveedor bajo pedido*)	**Mercado más barato.** (*El vendedor se está ahorrando una serie de costes, que presuntamente deben reflejarse en el precio*)
Artículos digitales con coste de distribución cero.	**Sin acosos por parte del vendedor.**
Contacto directo con el cliente. (*A través del correo electrónico*)	
Mayor eficiencia de las transacciones.	
Facilidad de *marketing* y soporte al cliente. (*Aprovechando las posibilidades del lenguaje html*)	
Mercado accesible para cualquier empresa. (*No son necesarias inversiones multimillonarias para realizar una buena página Web*)	

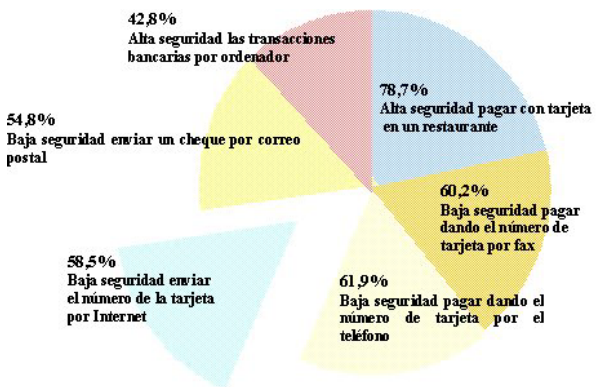
2. ¿QUÉ PROBLEMAS DE SEGURIDAD PRESENTA EN LA ACTUALIDAD?

Pero a pesar de estas ventajas innegables no debemos olvidar que el comercio electrónico – como toda actividad relativamente novel - presenta una serie de problemas, que al menos en la actualidad aún no están totalmente solucionados. Como muestra hagamos un pequeño análisis de la problemática que ha presentado la campaña de Navidad 98-99 en España, en cuanto a las transacciones comerciales realizadas a través del comercio electrónico:

- **Pedidos que no llegan dentro del periodo acordado**, normalmente por problemas de *stock*.
- **Pedidos que llegan en mal estado**. No nos debemos olvidar que salvo los productos digitales (s*oftware*), el resto de los pedidos se distribuyen mediante los canales tradicionales.
- **Pedidos que no llegan**.
- **Transacciones irrealizables**.
- **Devoluciones que no se reembolsan**, a pesar de la promesa de devolver el dinero si no se esta satisfecho con el producto.
- **Productos que no cumplen lo anunciado**, que entran de lleno en lo que se denomina "*publicidad engañosa*".
- **Síndrome de "*la muerte en un millón de clics*"**, páginas en las que la navegación se convierte en un suplicio insufrible, por su diseño, extensión o dificultad de acceso a la información que interesa.
- **Lentitud de la red,** todos los internautas conocemos el "*suplicio*" que supone el esperar a que se cargue una página Web. Por no hablar de la falta de una tarifa plana.

Esta problemática es real y afecta a las partes que tienen algún papel en comercio electrónico. Pero existe otro problema, quizás menos aparente, pero igualmente existente. ¿Son seguras estas transacciones? ¿Qué ocurre cuando envío mi número de tarjeta de crédito por la Red? ¿Es segura las Red para el desarrollo del comercio electrónico? ¿Es posible que alguien se haga con mi número de tarjeta de crédito y se apodere de mi dinero?

Según la EGM en su segunda encuesta sobre Internet (www.aimc.es/aimc/html/inter/informe.html), los encuestados piensan que operar con medios electrónicos, o no, de pago, ofrece los siguientes grados de seguridad.



Como vemos, el hecho de tener un "*cierto control físico*" sobre el instrumento de pago, - caso de pagar con tarjeta en un restaurante - determina un grado de confianza mayor que el que merece en la realidad, mientras que el 58,5% de las personas preguntadas opina que la Seguridad en Internet es baja.

En cualquier caso, una transacción electrónica está expuesta a una serie de posibles ataques:

- **Ingeniería social**, que no es otra cosa más que el termino moderno de algo tan viejo como la propia humanidad: El timo.
- **Empleados desleales** en la empresa del vendedor.
- ***Carding***, o generación de números falsos de tarjeta de crédito.
- **Hackers**, que intercepten las comunicaciones o entren en los servidores, con el fin de apoderarse de números de tarjeta de crédito o palabra de paso (*password).*

Además, en la vertiente lógica y en función de la robustez de los sistemas operativos, existen otra serie de problemas, como pueden ser:

- Riesgos de seguridad del *server*. (*Bugs*, CGI´s, mala configuración, malas políticas de seguridad, permisos a usuarios locales, espacio compartido FTP-WWW, listados automáticos de directorios, enlaces simbólicos, etc.)
- Riesgos de seguridad del cliente. (Navegadores, JAVA, *applets* maliciosas, etc.)
- Problemas de seguridad de la comunicación: falta de confidencialidad, integridad, disponibilidad y autenticación.
- Problemas de virus, virus de macro, Caballos de Troya, etc.
- Problemas de acceso a archivos del ordenador, denegación de servicios, borrado de información, etc.

Lo que está claro es que, y dado el sistema de funcionamiento de la Red, la seguridad de la transacción depende de la seguridad de las comunicaciones, lo que nos lleva a la siguiente pregunta: ¿son seguras las comunicaciones? Cuando navegamos por la Red dejamos un rastro compuesto por el nombre y dirección de la máquina, sistema operativo y navegador utilizado, página Web anteriormente visitada y solicitada y en ocasiones, dirección de correo electrónico. Si no tenemos la opción de las "galletitas", las famosas *cookies* desactivada en nuestro navegador la información puede ser más personalizada. Un ejemplo de esto lo tenemos en la página Web de Gonzalo Álvarez Marañón (http://www.iec.csic.es/criptonomicon), que conviene visitar y en la que probablemente nos llevaremos alguna sorpresa.

La problemática que la Red presenta para el autor Técnico-Científico y Académico, también es clara aunque desgraciadamente no tanto como la solución. Al ser Internet una red abierta - y debido a la propia naturaleza de los canales digitales -, cualquier página Web, trabajo publicado electrónicamente, dibujo, gráfico, etc., es susceptible de ser copiado por una persona, que puede arrogarse su autoría incluyéndola en publicaciones electrónicas o en su propia página Web.

Una de las medidas de seguridad tomadas para proteger la propiedad intelectual, principalmente de los gráficos y dibujos es la inclusión de las denominadas "*marcas de agua*" que permitan asociar a un autor determinado e identificar como suya cualquier imagen que éste haya generado. Para cumplir esta función de propiedad se deben cumplir los siguientes puntos:

1. Que sea imperceptible. A simple vista no debe apreciarse su existencia.
2. Solamente debe poder haber sido incluida por aquella persona que la utiliza en su defensa (el autor).
3. Debe ser hereditaria. Cualquier copia realizada debe incluir esta marca.

Esta protección debe ser introducida ante notario, o lo que es más fácil, gestionada por una empresa digital (como por ejemplo *Digimarc* incluida en el programa gráfico *Photoshop 5.0*,), que almacene el ID del creador, asociando la imagen a una persona y a una fecha determinada e incluyendo estas referencias en su base de datos.

En cuanto a los trabajos escritos pueden utilizarse programas como *Acrobat Distiller*, que permiten introducir posibilidades como: permitir - o no - su impresión, cambios, copiar texto o imágenes, añadir notas, etc., y que informan sobre quien es el autor, así como la fecha en que lo ha realizado.

3. ¿QUÉ SOLUCIONES EXISTEN?

En primer lugar hay que definir que requisitos se exigen para mantener con seguridad todas las operaciones que conlleva la propia existencia del comercio electrónico:

- Autenticación.
- Integridad (involuntaria y/o voluntaria).

- Confidencialidad.
- Prueba de la transacción.
- Gestión de riesgo y autorización.
- Disponibilidad y fiabilidad.

Para dar respuesta a estas necesidades de seguridad, en la actualidad se utilizan los siguientes elementos:

- Existencia de números PIN (*Personal Identificación Number*), como el caso de las tarjetas de banda magnética que nos permiten operar los cajeros electrónicos.
- Existencia de protocolos de cifrado de autenticación.
- Códigos de autenticación de mensajes (MACs), funciones resumen (HASH) y firmas digitales para garantizar la integridad de los datos durante las fases de almacenamiento, transmisión y recepción.
- Portar la tarjeta (caso de los monederos electrónicos, tarjetas de débito, etc.) y permitir su identificación mediante otros documentos (DNI, etc.).
- Existencia de dispositivos con capacidad de cálculo: PCs, tarjetas inteligentes, etc., que impidan –posteriormente - el repudio de la operación.
- Tarjetas que pueden ser inteligentes, tarjetas donde se archivan algoritmos de cifrado, o tarjetas que contienen microprocesadores , bandas magnéticas, etc.
- Técnicas de cifrado, para mantener la información a salvo de todos, a excepción del emisor y el receptor legales de la misma y que permiten garantizar que el pago se ha realizado.
- Medios de identificación antropométricos, basados en la confirmación de una característica física personal e infalsificable.

De todas las técnicas anteriormente mencionadas, las únicas que ofrecen una garantía de seguridad son las de cifrado, y que como veremos más adelante, no solamente van a servir para cifrar los datos, si no que nos van a permitir una explotación de sus posibilidades más amplia.

4. ¿CUÁL ES LA SOLUCIÓN IDÓNEA? ¿LAS TÉCNICAS DE CIFRADO?

El cifrado – básicamente - consiste en convertir un texto - o dato – claro (legible) en un texto irreconocible, utilizando para ello un algoritmo de cifrado. Para convertir el texto irreconocible en un texto o dato de nuevo comprensible, hará falta disponer de una clave. Así mismo permite validar la información intercambiada y dar seguridad a las comunicaciones.

Las técnicas de cifrado tratan de asegurar que:

- Sólo el receptor debe ser capaz de acceder a los datos en claro (confidencialidad).
- Nadie ha podido añadir, quitar o cambiar los datos originales del mensaje, o los que puedan acompañarlo (integridad).
- El mensaje - o los datos - provienen de quien dice ser (autenticación).

Para lograrlo existen dos grandes grupos de algoritmos de cifrado: los **sistemas simétricos**; en los que se utiliza la misma clave para cifrar y descifrar. (*Sistemas de clave privada*) y los sistemas **asimétricos**; en los que la clave de cifrado y la de descifrado son distintas. (*Sistemas de clave pública).*

Las técnicas de cifrado también se utilizan para generar dos elementos básicos para lograr la autenticación de las partes mediante:

- Las **firmas digitales** que consiguen el *no repudio y la autenticación*. Se entiende por firma digital al conjunto de datos que se añaden a una información para protegerlos contra falsificaciones y que permiten al

receptor probar la fuente e integridad de los mismos, utilizando para ello parte de la clave secreta del firmante y la elaboración de un valor de control cifrado (función *hash*).

- **Autoridades de Certificación (AC)**. La función de las AC es autenticar a los participantes en una transacción o comunicación ya que el empleo de canales inseguros, no garantiza el aspecto económico de la transacción. Cualquiera puede suplantar a otra persona introduciendo correctamente los datos de su tarjeta. La pregunta surge instantáneamente: ¿Cómo autentican las AC? Mediante los certificados, o lo que es lo mismo, una clave electrónica formada a partir de la clave pública del cliente, firmada y certificada por la clave privada de la AC. Un certificado tiene los siguientes campos:
  - Identificador de a quién pertenece el certificado.
  - Identificador de la AC.
  - Fechas de inicio y finalización de validez del certificado.
  - Identificador o número de serie.
  - Clave pública del cliente a quien se está certificando.
  - Firma de la AC.

Con la finalidad de alcanzar el mayor grado de seguridad en las transacciones se utiliza el modelo de referencia que está recogido en el marco OSI. Parte 2ª. Arquitecturas de seguridad: *Information Processing Systems. OSI Reference Model - Part 2: Security Arquitecture*", ISO/IEC IS 7498-2, que arropa los siguientes servicios: Autenticación, control de accesos lógicos al sistema, confidencialidad de los datos, integridad de los datos y no repudio de los mismos, que se realiza mediante envíos con prueba de origen y prueba de entrega.

Los servicios que se recogen son los siguientes:

- **Cifrado**, que puede realizarse mediante el uso de sistemas de cifrado simétricos o asimétricos y que puede aplicarse extremo a extremo o a cada enlace del sistema de comunicaciones. El mecanismo de cifrado debe soportar el servicio de confidencialidad de los datos y puede complementar a otros mecanismos para conseguir diversos servicios de seguridad.
- **Firmado digital**: El mecanismo de cifrado digital soporta los servicios de integridad de los datos, autenticación del emisor y no repudio con prueba de origen. Para que se pueda proporcionar el servicio de no repudio con prueba de entrega, hay que forzar al receptor para que envíe un acuse de recibo firmado digitalmente.
- **Control de acceso**, que se usa para autentificar las capacidades de una entidad para acceder a un recurso dado. El control de acceso se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación.

También se garantiza la **integridad de datos**. Aquí hay que distinguir entre la integridad de una unidad de datos individual y la integridad de una secuencia de unidades de datos. Para lograr integridad de una unidad de datos, el emisor añade datos suplementarios a la unidad de datos. Estos datos suplementarios se obtienen en función de la unidad de datos y, generalmente, se cifran. El receptor genera los mismos datos suplementarios a partir de la unidad original y los compara con los recibidos.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, algún mecanismo de ordenación, tal como el uso de números de secuencia, un sello temporal o un encadenamiento cifrado entre las unidades.

Otro concepto importante es el de intercambio de autenticación, que tiene dos grados:

- **Autenticación simple**: el emisor envía su identificador y una contraseña al receptor, el cual los comprueba.
- **Autenticación fuerte**: utiliza propiedades de los sistemas de cifrado de clave pública. Un usuario se autentica mediante su identificador y su clave privada. Su interlocutor debe verificar que aquel, efectivamente, posee la clave privada, para lo cual debe obtener, de algún modo, la clave pública del primero. Para ello deberá obtener su certificado. Como ya hemos visto, un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el periodo de tiempo determinado, que asocia una clave pública a un usuario determinado.

5. ¿CUÁLES SON LOS ESTÁNDARES DE SEGURIDAD EN EL COMERCIO ELECTRÓNICO?

Los estándares de seguridad vienen marcados por los sistemas de pago utilizados en Internet, y que fundamentalmente son: Sistemas de pago anticipado. (*Pay Before*), sistemas de pago inmediato, contrareembolso. (*Pay now*) y sistemas de pago posterior, domiciliación. (*Pay after*). En cualquier caso, hay que tener en cuenta que un pago realiza-

do a través de Internet, sin protocolos de seguridad, se lleva a cabo a través de un canal inseguro o potencialmente inseguro.

Los estándares de seguridad que actualmente se encuentran operativos en la son:

- **TIS/PEM**: Para plataformas UNIX, VMS, DOS y Windows.
- **RIPEM**: Que carece de certificados de autenticación de clases y cuya exportación está prohibida fuera de los EE.UU. Esta implementación cuenta con el apoyo del gobierno estadounidense.
- **PGP**: Que proporciona autenticación y confidencialidad.
- **S/MIME**: Cuya finalidad es proporcionar los servicios de confidencialidad, integridad, no repudio de origen y autenticación. Como ejemplo de la inseguridad que presentan los protocolos frente a los ataques de la comunidad de internautas valga el ejemplo de la noticia recogida en el Boletín Criptonomicón Nº 32, bajo el titulo "S-MIME, DESCIFRADO EN POCOS DÍAS": Santiago Nuñez, santi@dilmun.ls.fi.upm.es, del laboratorio de criptografía de la Facultad de Informática de Madrid ww.fi.upm.es ha logrado romper y descifrar un mensaje RC2 de 40 bits, que es el que usa NetScape. Se puede consultar información de cómo lo hizo en: www.fi.upm.es/ccfi/noticias/smime.html
- **PKCS**: Que trata de garantizar, fundamentalmente, la interoperatibilidad entre sistemas de clave pública, en cuanto a cifrado se refiere.
- **SSL**: Conjunto de protocolos diseñados por Netscape.
- **SET**: Patrocinado por las principales empresas.

Dada la orientación de este artículo, dirigida hacia el comercio electrónico, vamos a ver únicamente las dos últimas propuestas para lograr su seguridad y la autenticación entre las partes, SSL y el SET, dado que un tercer protocolo que se presentó con la misma finalidad, HTPP propuesto por Commerce Net, está prácticamente desechado, en la actualidad, para dar seguridad a las transacciones electrónicas. Tanto SSL como SET requieren de la existencia de compatibilidad entre el navegador y el servidor para que sean operativos.

El primero de ellos SSL (*Secure Socket Layer*), es la propuesta aportada por Netscape Communications Corporation en el año 1994. SSL se ubica a nivel de pila OSI, entre los niveles de transporte TC/IP y de aplicación, donde se encuentran los protocolos HTTP, FTP, SMTP, Telnet, etc., lo que le permite securizar, con mínimos cambios, en el programa que utilice TCP. Principalmente ofrece los siguientes servicios:

- Autenticación del servidor.
- Cifrado de datos en tránsito.
- Autenticación del cliente (opcional).
- Confidencialidad.
- Integridad.
- Interoperatibilidad entre máquinas.
- Extensibilidad.
- Creación de un canal seguro.

Los navegadores que lo soportan son: Netscape Navigator 3.0, Secure Mosaic, Microsoft Internet Explorer 3.0 y/o versiones superiores de los citados navegadores. En cuanto a los servidores que le dan cobertura son Netscape, Microsoft, IBM, Quaterdeck, OpenMarket, O´Reilly and Associates.

SSL utiliza **certificados X.509** para el intercambio de claves públicas. Estos certificados X.509 contienen además de la clave pública del interlocutor, información acerca de su identidad, así como información complementaria sobre algoritmos utilizados para la generación de claves, plazos de validez del propio certificado, etc. Por otra parte, estos certificados contienen una firma digital que garantiza la integridad de sus contenidos, ya sea por la clave privada del mismo interlocutor (**certificados autofirmados**), o por la clave privada de una tercera parte (**certificado firmado por una CA**). Son los de este último tipo, los firmados por una CA, los necesarios para garantizar los cuatro requerimientos iniciales.

Los datos de un sujeto que se incluyen en un certificado X.509 son:

- CN: Nombre común o nombre largo.
- E-MAIL: Dirección de correo electrónico.
- O: Nombre de su organización.

- OU: Departamento.
- L: Localidad.
- SP: Provincia o estado.
- C: País.

SSL lucha en la actualidad por la primacía y pretende ser un canal seguro. Gráficamente su forma de trabajar es la siguiente:

Durante la negociación que se establece entre el servidor cliente (a través de su navegador) y el servidor seguro se negocian los siguientes contenidos:

- Elección de algoritmos, seleccionando dos que sean compatibles y lo más fuertes posibles.
- Autenticación, entre uno y otro.
- Generación de clave de sesión, para autentificarla.
- Verificación de canal seguro, entre el cliente y el servidor.

En el navegador Internet Explorer 5 el uso de SSL se selecciona desde la ventana "Propiedades de Internet", que se muestra a continuación. Es de señalar que si pulsamos en el menú "Ayuda" vemos una nueva ventana que nos informa con qué intensidad de cifrado está trabajando el navegador - 40 bits -, en aplicación de la normativa norteamericana ITAR (*International Traffic in Arms Regulations*), que prohibe la exportación de aplicaciones de cifrado con 128 bits o más, autorizando únicamente la exportación de aplicaciones con 40 o 56 bits de longitud de clave, excepto en

ocasiones muy especiales, fundamentalmente en aplicaciones para empresas norteamericanas fuera de EE. UU., o entidades de crédito. Actualmente se considera que la longitud mínima – exclusivamente desde el punto de vista de la seguridad - para ofrecer garantías de seguridad es de 90 bits

SSL se basa en que el navegador verifica la clave pública certificada enviada por el servidor seguro, que esta clave está firmada por una Autoridad de Certificación (CA) y que está integrada en el navegador. SSL permite también la elección del sistema de cifrado a utilizar. En definitiva SSL proporciona un canal seguro practico y fácil de instalar, pero adolece de los siguientes problemas:

- Longitud de clave pequeña (40 bits en Europa).
- Sólo protege transacciones entre dos partes: servidor Web comercial y navegador del comprador. Pero en caso de pago con tarjeta, existen tres partes: comprador, vendedor y emisor de la tarjeta.
- Un comerciante deshonesto puede utilizar ilícitamente la tarjeta.
- El comerciante corre el riesgo de que la tarjeta sea falsa, o que ésta no haya sido aprobada.
- Vulnerabilidad de PKCS1 (*Public Key Cryptography Standard*) que puede surgir del intercambio de claves.
- También los servidores con Windows NT y la opción SSL activada, son susceptibles de recibir un ataque de denegación de servicio al no poder distinguir entre páginas que requieren SSL y las que no.

Una ventaja innegable de SSL es su sencillez de utilización para cualquier usuario que quiera realizar una transacción desde su casa, ya que su utilización es transparente para él.

Otra propuesta es SET (*Secure Electronic Transaction*), desarrollado en el año 1995 por VISA y MasterCard y que actualmente está apoyado por MICROSOFT, NETSCAPE, IBM y VERISIGN además de las compañías desarrolladoras, y que pretende, a través del cifrado, garantizar la confidencialidad de la información, tanto la económica, como la referente a los bienes adquiridos. SET asegura la integridad de los pagos, autentica el binomio cliente/vendedor y puede utilizar diferentes plataformas tanto de *hardware* como de *software*.

¿Cómo opera? Utiliza el actual sistema de tarjetas de crédito, sustituyendo las transacciones físicas por transacciones electrónicas. Gráficamente presenta el siguiente aspecto:

SET ofrece los siguientes servicios:

- **Autenticación:** Todas las partes involucradas en la transacción pueden autenticarse mediante certificados digitales. Se evitan así fraudes en las tarjetas o la falsificación de los centros de compras y permite al Banco verificar las identidades del comprador y el vendedor.
- **Confidencialidad:** Se cifra el número de la tarjeta. Si se quiere proteger el resto de la información, habrá que recurrir a SSL.
- **Integridad:** Garantizando que los datos intercambiados no podrán ser alterados.
- **Gestión de pago:** Al gestionar tareas asociadas; registro del comprador y vendedor, autorizaciones, liquidaciones, etc.

Pero SET también representa una serie de problemas, que pueden resumirse en los siguientes puntos:

- Necesita un *software* especial, tanto para el comprador (monedero), como para el vendedor (POST o TPV), que se está desarrollando lentamente.
- Problemas de compatibilidad entre diferentes productos que presuntamente cumplen las especificaciones SET.
- Trámites engorrosos para clientes y comerciantes al requerir rígidas jerarquías de certificación lo que conlleva adquirir certificados distintos para diferentes tarjetas y trámites desconocidos para gran parte de los clientes.

Posiblemente, una vez se solucionen estos problemas, y sobre todo, sea más transparente para el usuario, de forma que no tenga que adquirir un certificado distinto para cada tramite, sea el del futuro, siempre que no salga al mercado electrónico un protocolo más seguro y flexible.

En España la Agencia de Certificación Española (ACE, http://www.ace.es) formada por Telefónica, SERMEPA, CECA y el Sistema 4B, ofrece el servicio de certificación SET desde finales del año 98.

Buscando otro tipo de soluciones también se han ideado esquemas de transacciones comerciales por la Web, que no necesitan sin transmitir números de tarjeta de crédito, ni información confidencial como por ejemplo:

- ***First Virtual Accounts***, que sólo se utiliza en la adquisición de servicios de Internet de precio bajo o medio.
- ***DigiCash,*** sistema análogo al del bonobus, diseñado para la adquisición tanto de servicios, como de bienes tangibles, que soporta el comercio interpersonal y permite canjearlo por dinero real en Bancos que soportan el sistema DigiCash.
- ***CyberCash***, utiliza cifrado fuerte para proteger los datos durante la transmisión, sin que la información quede depositada en ninguna parte. Requiere instalar *software* cliente y servidor.

Y para finalizar recojo una serie de consejos de la Agencia de Protección de Datos, que no tienen otra finalidad que la de comprar en la Red con la suficiente seguridad:

- Utilice, siempre que sea posible, las últimas versiones de los programas navegadores, ya que cada vez suelen incorporar mejores medidas de seguridad. Considere la posibilidad de activar en dichos programas las opciones que alerten sobre los intercambios de datos no deseados y no rellene aquellos datos que no desee hacer públicos (por ejemplo, dirección de correo electrónico, nombre, apellidos, etc.).
- No realice transacciones comerciales electrónicas a través de proveedores con sistemas "*inseguros*" o no fiables. Consulte el manual de su navegador para averiguar cómo informa de que se ha establecido una conexión con un servidor seguro.
- Recuerde que existen sistemas de dinero electrónico que preservan el anonimato de sus compras en Internet.
- Utilice los mecanismos de seguridad que tenga a su alcance para proteger sus datos de accesos no deseados. El medio más fiable para conseguirlo es el cifrado de los mismos.
- Salvo que se utilicen mecanismos de integridad, autenticación y certificación (firma digital, notarios electrónicos, etc.) no confíe ciegamente en que la persona u organización que le remite un mensaje es quien dice ser y en que el contenido del mismo no se ha modificado, aunque esto sea así en la inmensa mayoría de las ocasiones.

- No entregue más información que la estrictamente necesaria para recibir el producto que ha comprado (normalmente no existe motivo para que deba responder con su renta anual o sus ideas religiosas).
- Nunca entregue datos confidenciales si no es a través de un servidor seguro (que utilice SSL).
- No envíe su número de tarjeta de crédito por correo electrónico.
- Compruebe rutinariamente los certificados de los sitios seguros a los que se conecte. De nada sirve SSL si no se toma en serio.
- Reclame sus derechos como consumidor:
  - Exija imágenes del producto que piense adquirir, al menos cuando sea relevante.
  - Exija información detallada y clara sobre los precios.
  - Exija información sobre la forma de envío y coste adicional.
  - Exija que le expliquen las condiciones de garantía y devolución.
  - Busque la página sobre política de privacidad del comercio, para saber qué se hace con su información privada, tanto la recopilada directamente, suministrada al rellenar formularios, como la obtenida indirectamente por tu navegación. Si no la encuentra, exíjala.
  - No pague en efectivo, ni con cheque, ni con tarjeta de débito, mejor hágalo con tarjeta de crédito. Es más seguro de lo que generalmente se cree y le ocasionará menos problemas en caso de irregularidades con la entrega de su compra o fraude con su tarjeta.
- Consulte con su banco las condiciones de resolución de disputas con el comerciante. La entidad financiera de medios de pago le respalda. En caso de fraude, el que tendrá problemas será el comercio en el que se hizo la compra con su tarjeta, y no usted.

CONCLUSIONES

A modo de pequeño resumen se pueden extraer las siguientes conclusiones para que el comercio electrónico se convierta en una alternativa real, y no sólo teórica o con un pequeño peso especifico en el tejido comercial mundial:

- Debe existir una protección efectiva del *copyright*.
- La seguridad y la privacidad son básicas para las operaciones a través de Internet.
- No se deben poner nuevos impuestos en Internet.
- Los padres y los consumidores deben tener herramientas eficaces para proteger a sus familias y su privacidad.
- Los gobiernos deben promover la competencia y la desregulación en todos los mercados de las telecomunicaciones.
- Las fuerzas del mercado, y no los gobiernos, deben dirigir la evolución de la autenticación electrónica.
- No debe permitirse que las barreras aduaneras afecten al comercio electrónico.
- Las empresas necesitan leyes claras, justas y sencillas para afrontar los contratos en línea.
- Así mismo, es necesario que exista una armonización legal, independientemente de los países donde estén situadas cualquiera de las partes, y que permitan acabar con una cierta impunidad, que existe en la actualidad.
- Se deben utilizar aplicaciones fuertes de cifrado, sean norteamericanas o europeas. En el primer caso pasa por la derogación de la parte de la normativa ITAR que afecta a la exportación de productos de cifrado. En el segundo, se debe autorizar la exportación a países situados fuera de la CEE.
- Las aplicaciones de seguridad deben ser seguras, flexibles e independientes de las plataformas y del *software* y ser totalmente transparentes para los usuarios.
- Los Gobiernos tienen que comprender la importancia de la utilización de aplicaciones de cifrado por parte de empresas y particulares, sin poner las trabas legales que existen en la realidad o que se quieren imponer en un futuro, olvidándose de las "*terceras partes de confianza*", (*Vg.: Articulo 52 de la Ley General de Telecomunicaciones, de 8 de abril de 1998*), de la prohibición de determinadas aplicaciones de cifrado, etc.
- Es necesario que se arbitren mecanismos de certificación que impidan el repudio de las transacciones electrónicas, y que estos instrumentos tengan la suficiente validez legal, como para proteger a las partes, a modo de firma ológrafa. España se ha situado a la cabeza con el proyecto de certificación CERES de la Fabrica Nacional de Moneda y Timbre, y la promulgación del Real Decreto Ley 14/1999, de 17 de septiembre de 1999, sobre la firma electrónica.
- Es esencial que los códigos de los sistemas operativos que soportan los servidores de comercio electrónico, sean abiertos. *Vg.: Linux*.
- Los algoritmo de cifrado que se utilicen para proteger las transacciones electrónicas deben seguir el principio de KERCKHOFFS.